UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/600,687	06/20/2003	Philip D. MacKenzie	15	6727

7590 06/15/2009

Ryan, Mason, & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560

EXAMINER	
TO, BAOTRAN N	
ART UNIT	PAPER NUMBER
2435	
MAIL DATE	DELIVERY MODE
06/15/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/600,687	**Applicant(s)** MACKENZIE, PHILIP D.	
	Examiner Baotran N. To	**Art Unit** 2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03/09/2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is in response to the Amendment filed 03/09/2009.

Claims 1-16 are pending for examination.

Response to Arguments

2. Applicant's arguments filed 03/09/2009 have been fully considered but they are not persuasive.

Applicant argues that “no where do the two Faucher terminals "jointly perform a decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares of a key that each party holds," as recited in the independent claims” (Page 3 of Remarks).

Examiner respectfully disagrees. Faucher expressly discloses terminal A sends its certificate to terminal B and terminal B sends its certificate to terminal A. Terminal A decrypts and validates terminal B's certificates using the KCA public decryption key. Similarly, terminal B decrypts and validates terminal A's certificate using the KCA public decryption key. Terminal A generates a secret random component R.sub.a, calculates the corresponding public component X.sup.R.sbsp.a mod P, encrypts it using the public encryption key PK.sub.b extracted from terminal B's certificate, and transmits PK.sub.b (X.sup.R.sbsp.a mod P) to terminal B. Terminal B generates a secret random component R.sub.b, calculates the corresponding public component X.sup.R.sbsp.b mod P, encrypts it using the public encryption key PK.sub.a extracted from terminal A's certificate and transmits PK.sub.a (X.sup.R.sbsp.b mod P) to terminal A. Terminal A receives and decrypts the message, obtains terminal B's public random component X.sup.R.sbsp.b mod P and exponentiates using its secret random component R.sub.a. The result modulus P is passed over the hash function to obtain the session key. Terminal B receives and decrypts the message from terminal A, obtains terminal A's public random component X.sup.R.sbsp.a mod P and exponentiates it using its secret random component R.sub.b. The result modulus P is passed over the hash function H to obtain the session key" (col. 8, lines 25-48). As explained above, Faucher discloses that terminal A and terminal B have to exchange their information such as secret random component R sub a and secret random component R sub b to generate the shared information session key to use this session key to decrypt the ciphertext (col. 2, lines 14-20 and col. 15, line 55 - col. 16, line 23; *decrypting messages exchanged between said node and said communicating terminal using said common session key*) which can read on the claim limitation jointly perform a decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares of a key that each party holds.

Applicant further argues, "Applicant maintains that the Examiner has failed to identify a cogent motivation for combining Cramer and Faucher in the manner proposed" (Page 4 of Remarks).

Examiner respectfully disagrees with this contention. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and In re Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992), In this case, Cramer's reference and Faucher's reference are analogous arts. They both specifically disclose to how to secure communications by using the cryptographic system that can support the motivation to combine the Cramer's teaching with Faucher's teaching to establish the limitations of Claim 1 that provides secure communications conducted over insecure channels (Faucher, col. 1, lines 13-15). Furthermore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Faucher's reference within Cramer to include wherein the assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext from the second party device to the first party device. One of ordinary skill in the art would have been motivated to do this because it would secure communications conducted over insecure channels using pubic-keys method (Faucher, col. 1, lines 13-15).

Applicant further argues Cramer does not teach or suggest “exchange of information between the first party device and the second party device whereby at least a portion of the information is encrypted using an encryption technique such that one party encrypts information using its own public key and another party cannot read the information but can use the information to perform an operation” (Page 5 of Remarks).

Examiner respectfully disagrees. Faucher further discloses wherein the generating step further comprises an exchange of information between the first party device and the second party device whereby at least a portion of the information is encrypted using an encryption technique such that one party encrypts information using its own public key and another party can not read the information but can use the information to perform an operation" (Faucher, Figure 5, col. 8, lines 8-55).

Applicant further argues that Cramer does not disclose or suggest "Cramer discloses generating a share of a random secret; generating information representing encryptions of a form of the random secret, a share of a private key, and the ciphertext; transmitting at least the encrypted information to the second party device; and computing the plaintext based at least on the share of the random secret, the share of the private key, the ciphertext, and the data received from the second party device" (Page 6 of Remarks).

Examiner respectfully disagrees. Cramer discloses generating a share of a random secret (Col. 7, lines 11-19); generating information representing encryptions of a form of the random secret, a share of a private key, and the ciphertext (Col. 7 lines 10-27) {private key Z, and the random group}; transmitting at least the encrypted information to the second party device (Col. 6, lines 46-57); and computing the plaintext based at least on the share of the random secret, the share of the private key, the ciphertext, and the data received from the second party device (Figure 3, Col. 9 lines 25-50).

Applicant further argues that Cramer does not disclose or suggest "the first party device and the second party device additively share components of a private key" and "generation and exchange of proofs between the first party device and the second party device that serve to verify operations performed by each party" (Page 6 of Remarks).

Examiner respectfully disagrees. Cramer discloses "the first party device and the second party device additively share components of a private key" in (Col. 7 lines 10-15, and Col. 9 lines 35-40); and generation and exchange of proofs between the first party device and the second party device that serve to verify operations performed by each party" in (Col. 8 line 38 to Col. 9 line 23).

For at least the above reasons, the rejections for claims 1-16 are respectfully maintained.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-2, 4-6, 8-9-10, 12-14, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cramer et al, (US Patent No. 6,697,488) hereinafter Cramer in view of Faucher (US Patent No. 5,515,441) hereinafter Faucher.

As per claims 1 and 9, Cramer discloses a method for use in a device associated with a first party for decrypting a ciphertext according to a Cramer-Shoup based encryption scheme (Col. 6 lines 10-15), the method comprising the steps of:

obtaining the ciphertext in the first party device sent from a device associated with a second party (Col. 8, lines 25-35, encrypted plaintext); and generating in the first party device a plaintext corresponding to the ciphertext based on assistance from the second device, the plaintext representing a result of the decryption according to the Cramer-Shoup based encryption scheme (Col. 8 line 25 to Col. 10 line 5) { Section IV teaches a verification steps to check the received ciphertext. Section V teaches steps of decrypting the received and verified ciphertext with the assistance of the sender} (Cramer and Shoup cryptographic system invention).

Cramer does not disclose "wherein the assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext from the second party device to the first party device, such that the first party device and the second party device jointly perform a decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares of a key that each party hold, but such that either can decrypt the ciphertext alone."

However, Faucher explicitly discloses wherein the assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext from the second party device to the first party device (col. 3, lines 5-50), such that the first party device and the second party device jointly perform a decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares of a key that each party hold, but such that either can decrypt the ciphertext alone (Figure 5, col. 8, lines 8-55).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Faucher's reference within Cramer to include wherein the assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext from the second party device to the first party device, such that the first party device and the second party device jointly perform a decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares of a key that each party hold, but such that either can decrypt the ciphertext alone. One of ordinary skill in the art would have been motivated to do this because it would secure communications conducted over insecure channels using pubic-keys method (col. 1, lines 13-15).

As per claims 8 and 16, Cramer discloses a method for use in a device associated with a first party for assisting in decrypting a ciphertext according to a Cramer-Shoup based encryption scheme, the method comprising the steps of:

receiving a request generated in and transmitted by a second party device for the partial assistance {*the partial assistance is the steps to verify the ciphertext before going through the decryption process in section V*} of the first party device in decrypting the ciphertext according to the Cramer-Shoup based encryption scheme (Col. 8, line 38 – Col. 9, line 25); and generating results in the first party device based on the partial assistance provided thereby for use in the second party device to complete decryption of the ciphertext" (Col. 8 line to Col. 10 line 5) { *Section IV teaches a verification steps to check the received ciphertext. Section V teaches steps of decrypting the received and verified ciphertext with the assistance of the sender*} (*Cramer and Shoup are the inventors of this prior art*) (Col. 8 line 25 to Col. 10 line 5).

Cramer does not disclose "wherein the assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext from the second party device to the first party device, such that the first party device and the second party device jointly perform a decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares of a key that each party hold, but such that either can decrypt the ciphertext alone."

However, Faucher explicitly discloses wherein the assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext from the second party device to the first party device (col. 3, lines 5-50), such that the first party device and the second party device jointly perform a decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares of a key that each party hold, but such that either can decrypt the ciphertext alone (Figure 5, col. 8, lines 8-55).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Faucher's reference within Cramer to include wherein the assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext from the second party device to the first party device, such that the first party device and the second party device jointly perform a decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares of a key that each party hold, but such that either can decrypt the ciphertext alone. One of ordinary skill in the art would have been motivated to do this because it would secure communications conducted over insecure channels using pubic-keys method (col. 1, lines 13-15).

As per claims 2 and 10, Cramer and Faucher disclose the limitations of Claims 1 and 9. Faucher further discloses wherein the generating step further comprises an exchange of information between the first party device and the second party device whereby at least a portion of the information is encrypted using an encryption technique such that one party encrypts information using its own public key and another party can not read the information but can use the information to perform an operation" (Faucher, Figure 5, col. 8, lines 8-55).

As per claims 4 and 12, Cramer and Faucher disclose the limitations of Claims 1 and 9. Cramer further discloses wherein the generating step further comprises:

generating a share of a random secret (Col. 7, lines 11-19);

generating information representing encryptions of a form of the random secret, a share of a private key, and the ciphertext (Col. 7 lines 10-27) {private key Z, and the random group};

transmitting at least the encrypted information to the second party device (Col. 6, lines 46-57); and

computing the plaintext based at least on the share of the random secret, the share of the private key, the ciphertext, and the data received from the second party device (Figure 3, Col. 9 lines 25-50).

As per claims 5 and 13, Cramer and Faucher disclose the limitations of Claims 1 and 9. Cramer further discloses wherein the first party device and the second party device additively share components of a private key" in (Col. 7 lines 10-15, and Col. 9 lines 35-40).

As per claims 6 and 14, Cramer and Faucher disclose the limitations of Claims 1 and 9. Cramer further discloses wherein the generating step further comprises generation and exchange of proofs between the first party device and the second party device that serve to verify operations performed by each party" in (Col. 8 line 38 to Col. 9 line 23).

4. Claims 3, 7, 11, and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cramer and Faucher and further in view of Ronald Cramer et al, "Multiparty Computation from Threshold Homomorphic Encryption".

As per claims 3 and 11, Cramer and Faucher disclose the limitations of Claims 1 and 9. Cramer and Faucher do not disclose "wherein the generating step further comprises an exchange of information between the first party device and the second party device whereby at least a portion of the information is encrypted using an encryption technique having a homomorphic property."

However, Ronald Cramer discloses wherein the generating step further comprises an exchange of information between the first party device and the second party device whereby at least a portion of the information is encrypted using an encryption technique having a homomorphic property (page 18).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Ronald Cramer's reference within Cramer and Faucher to include the encryption technique having a homomorphic property. One of ordinary skill in the art would have been motivated to do this because it would secure communications conducted over insecure channels (col. 1, lines 13-15).

As per claims 7 and 15, Cramer and Faucher disclose the limitations of Claims 1 and 9. Cramer and Faucher do not disclose wherein the proofs are consistency proofs based on three-move SIGMA-protocols.

However, Ronald Cramer discloses wherein the proofs are consistency proofs based on three-move SIGMA-protocols the proofs are based on three move SIGMA. Protocols (page 13).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Ronald Cramer's reference within Cramer and Faucher to include the proofs are based on three move SIGMA. protocols. One of ordinary skill in the art would have been motivated to do this because it would secure communications conducted over insecure channels (col. 1, lines 13-15).

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Contact Information

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Baotran N. To whose telephone number is (571)272-8156. The examiner can normally be reached on Monday-Friday from 8:00 to 4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/B. N. T./
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435